

FIG. 2

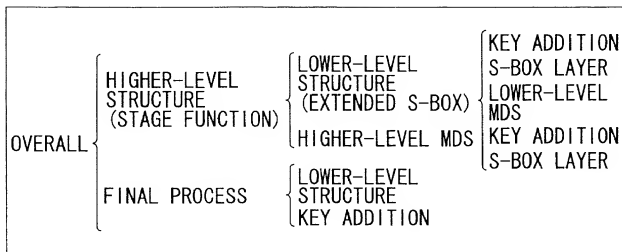


FIG. 3

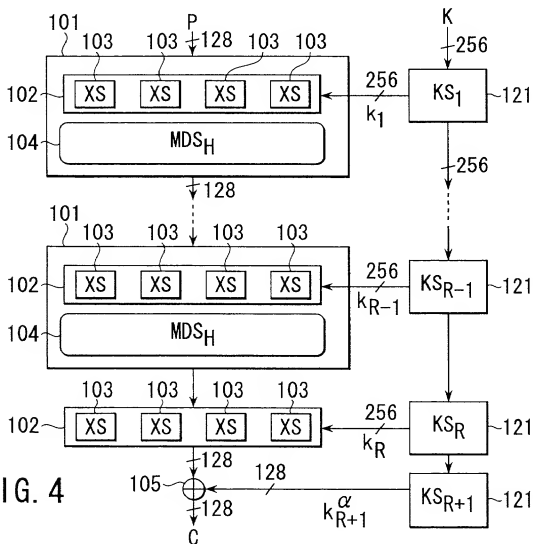


FIG. 4

$s[256]=\{$

72	AA	49	16	1E	3A	43	AE	66	BC	00	73	79	3B	FB	9F
69	6A	A2	50	6E	F5	EF	AC	22	02	AD	26	E2	DF	97	F0
9E	BF	17	8B	FA	7C	F4	71	7F	CA	F6	52	FD	C3	E5	64
53	8D	E0	F3	0F	78	CB	9B	68	3C	0D	1F	89	B6	EB	F7
44	4A	06	A6	56	6B	85	01	30	88	51	31	9C	A0	A3	25
60	5B	FF	05	B7	91	15	B3	A9	20	03	2B	61	42	95	4D
F9	7E	0E	E9	D8	F1	46	99	CE	BE	D9	54	80	B0	D2	4F
7A	E8	35	92	1B	7B	12	D6	4C	D5	E7	EE	B1	24	DE	21
04	10	AB	29	9A	81	FE	A7	B8	63	28	0A	8A	D1	C6	07
B9	C8	98	82	74	9D	84	47	94	C7	6C	11	D7	BA	C1	C9
DD	77	39	2F	2E	C2	67	41	E4	58	34	CD	1C	93	96	7D
2C	F8	B5	70	14	08	DC	CC	87	D0	5E	32	C5	C4	59	3E
CF	55	5C	23	75	2D	2A	86	4B	1D	5F	E6	FC	B2	4E	09
27	AF	19	B4	BD	6D	3D	6F	ED	62	EA	F2	D3	36	38	DB
BB	83	45	37	A4	EC	8C	5D	E1	33	90	A1	40	8E	1A	A5
0B	3F	5A	DA	13	76	0C	C0	48	E3	65	A8	18	8F	D4	57

$\}$

FIG. 5

112

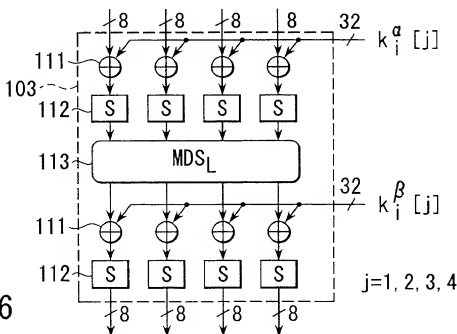


FIG. 6

FIG. 7

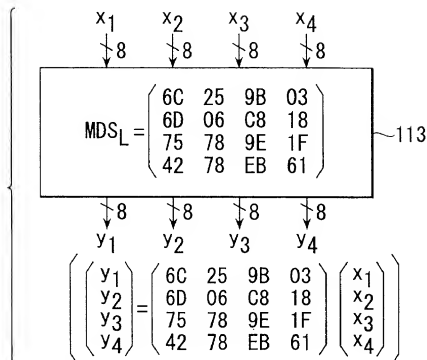


FIG. 8

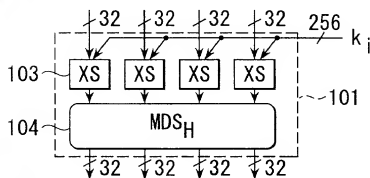
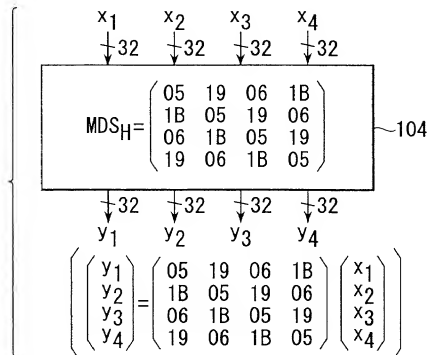
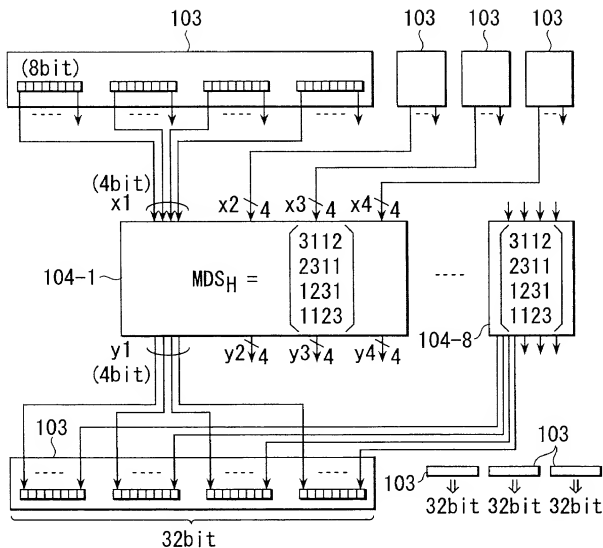


FIG. 9





$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 3112 \\ 2311 \\ 1231 \\ 1123 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

FIG. 10

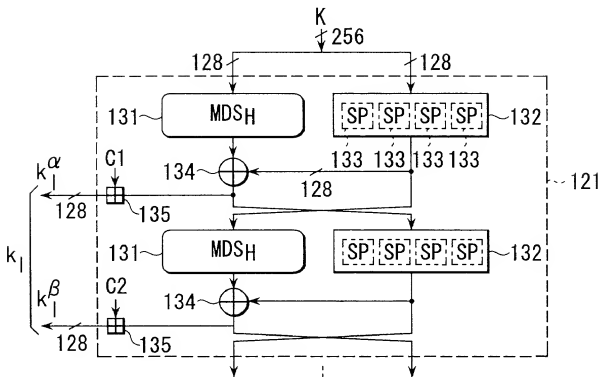


FIG. 11

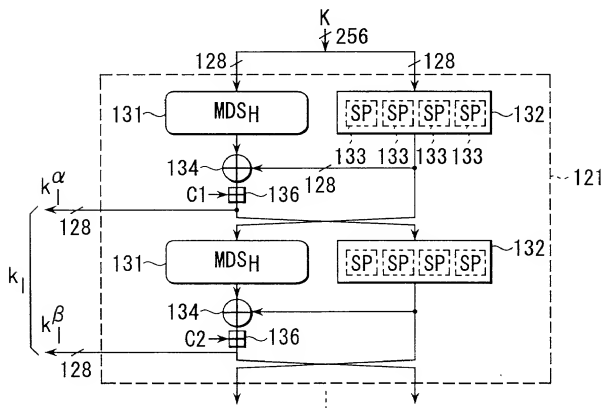


FIG. 12

FIG. 13

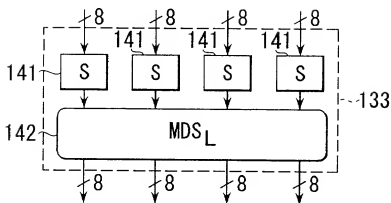


FIG. 14

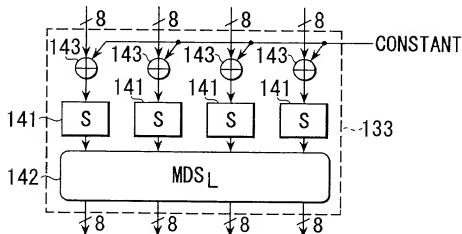


FIG. 15

C1	( H2, H0, H1, H1 )
C2	( H3, H2, H0, H3 )
C3	( H1, H0, H0, H0 )
C4	( H1, H0, H1, H3 )
C5	( H0, H1, H0, H2 )
C6	( H3, H2, H0, H0 )
C7	( H1, H2, H1, H0 )
C8	( H2, H1, H2, H3 )
C9	( H2, H1, H0, H0 )
C10	( H1, H1, H1, H2 )
C11	( H3, H1, H1, H2 )
C12	( H1, H1, H2, H0 )
C13	( H1, H3, H3, H1 )
C14	( H2, H3, H3, H1 )
C15	( H1, H3, H1, H0 )
C16	( H1, H0, H0, H3 )
C17	( H1, H2, H0, H3 )

WHERE

$$H0 = (5A827999)_H$$

$$= \sqrt{2}/4 \times 2^{32}_J$$

$$H1 = (6ED9EBA1)_H$$

$$= \sqrt{3}/4 \times 2^{32}_J$$

$$H2 = (8F1BBCDC)_H$$

$$= \sqrt{5}/4 \times 2^{32}_J$$

$$H3 = (CA62C1D6)_H$$

$$= \sqrt{10}/4 \times 2^{32}_J$$

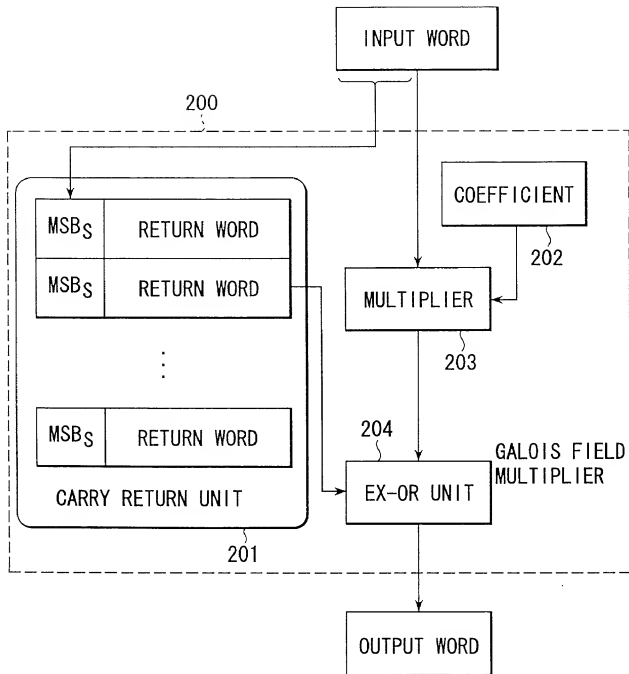
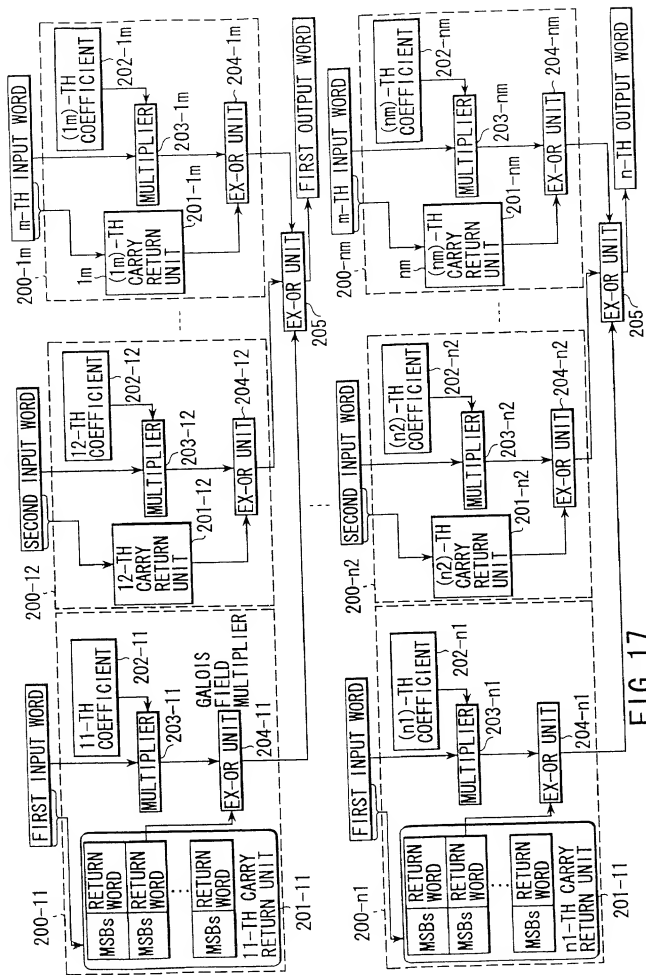


FIG. 16





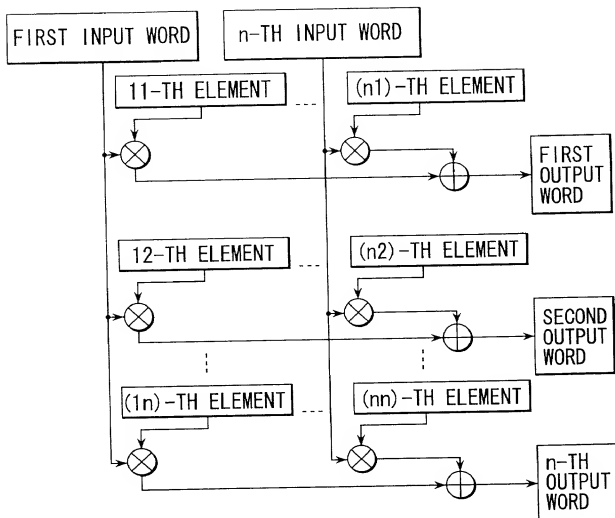


FIG. 18

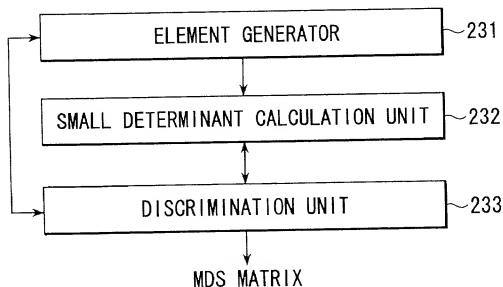


FIG. 19

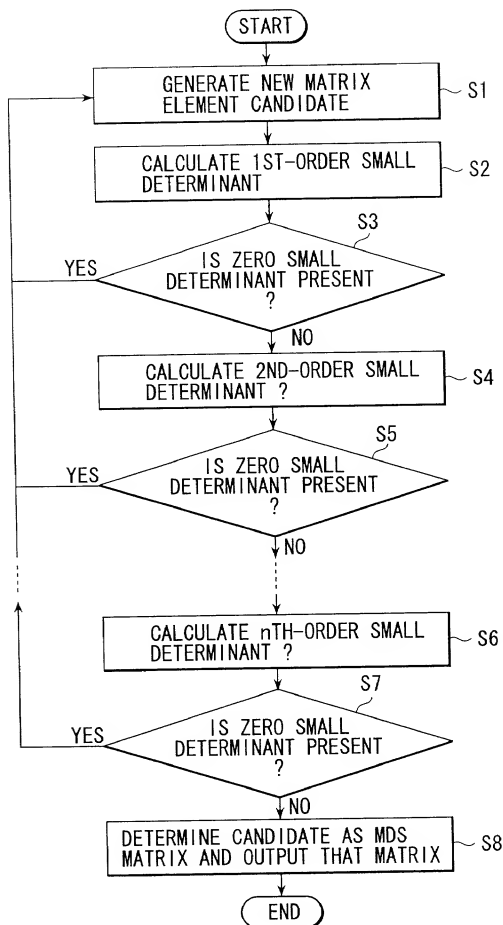


FIG. 20

FIG. 21

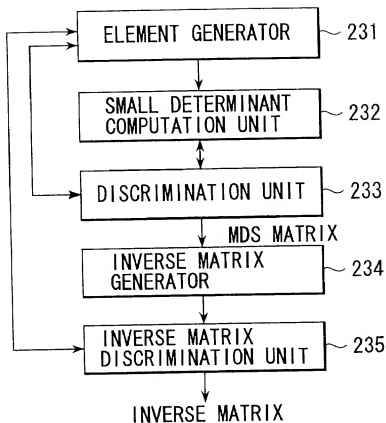
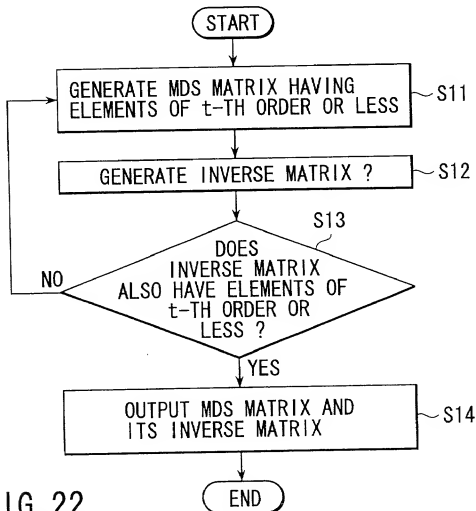


FIG. 22



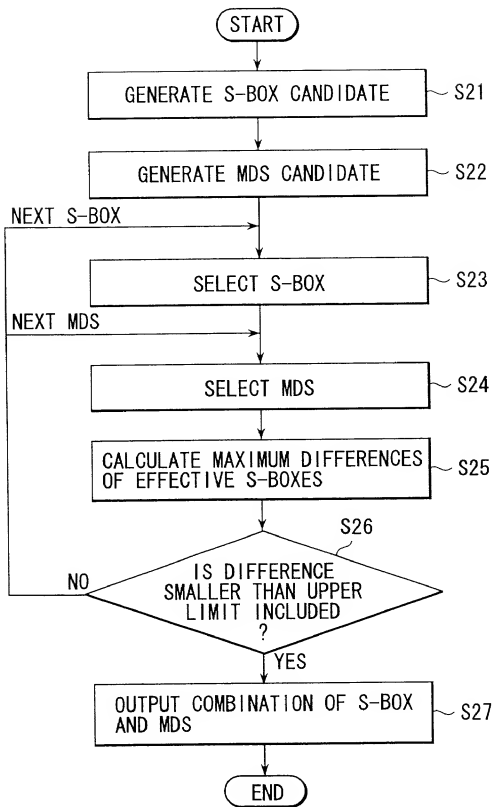


FIG. 23

FIG. 25

FIG. 26

FIG. 27

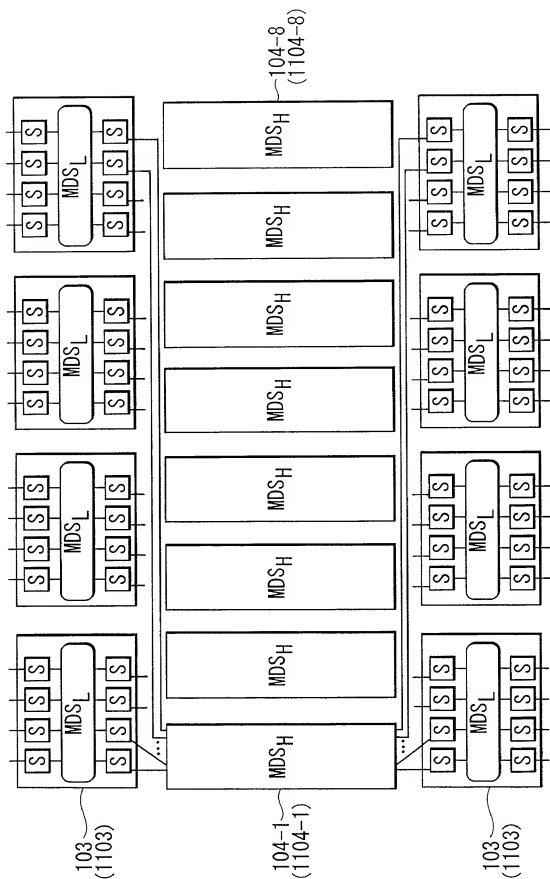


FIG. 28



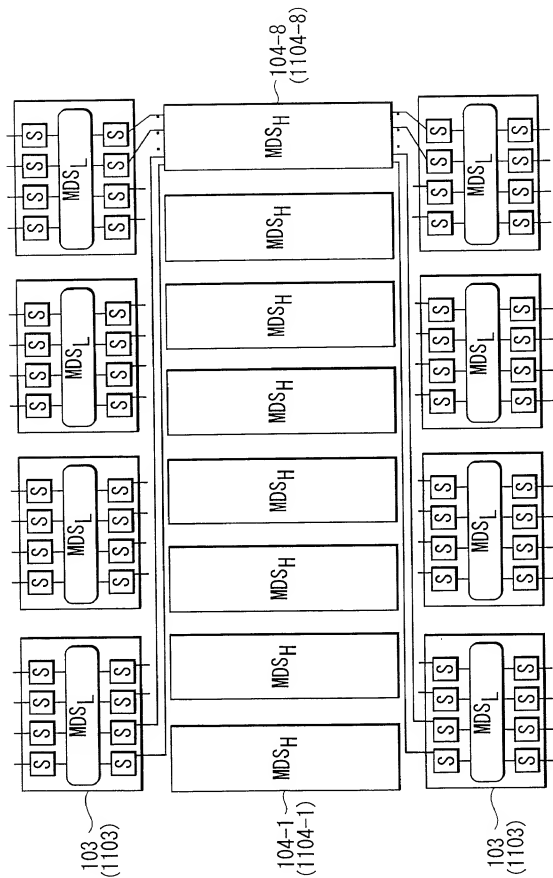


FIG. 29

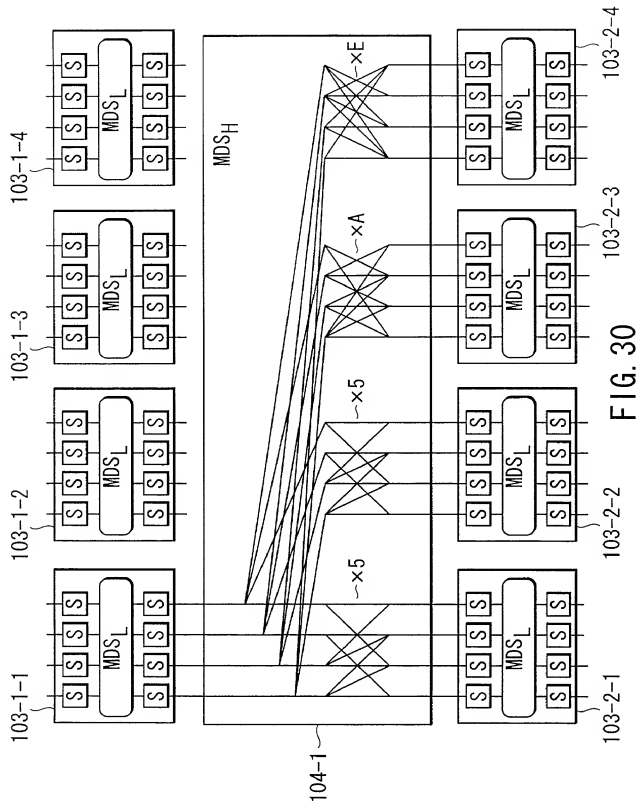
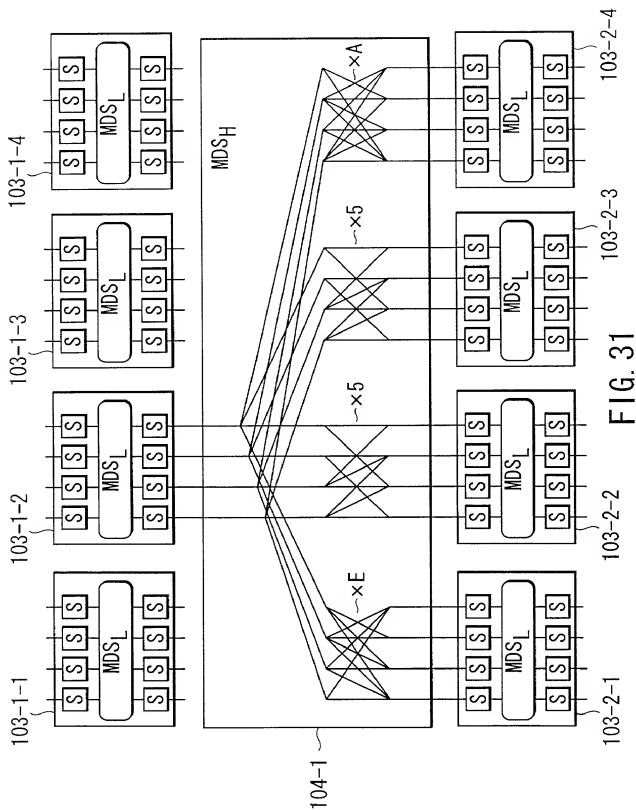


FIG. 30



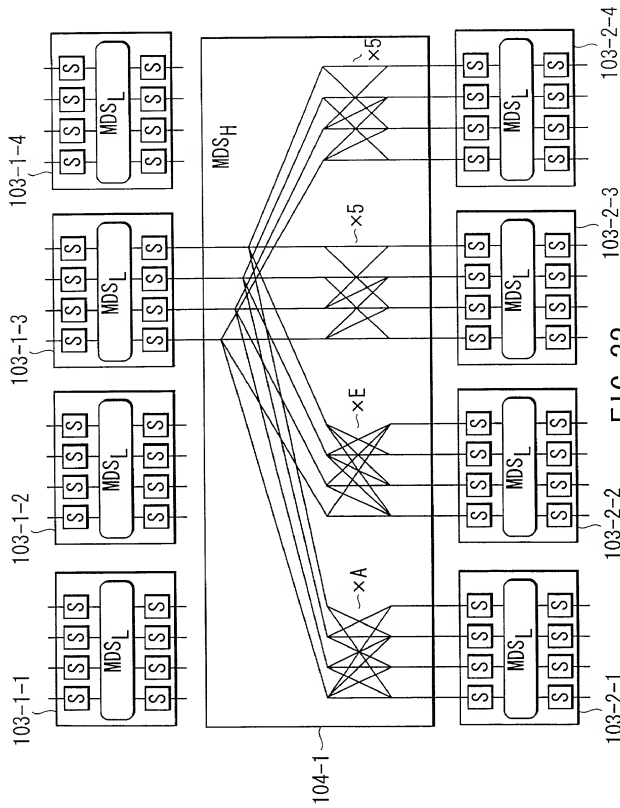
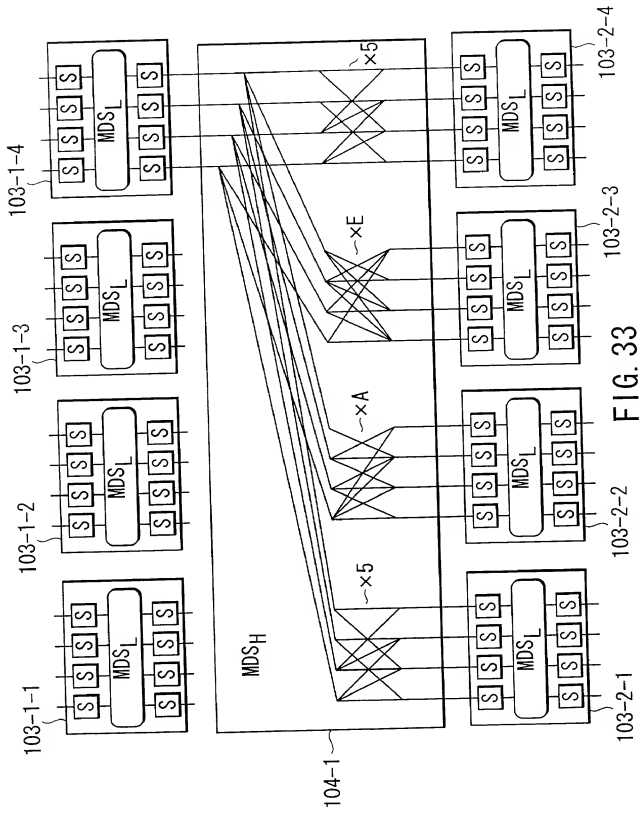
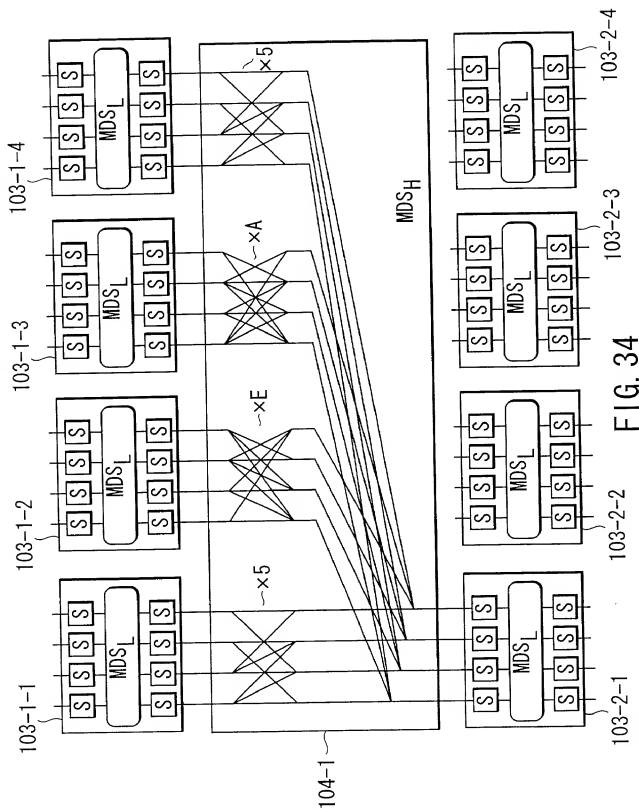


FIG. 32





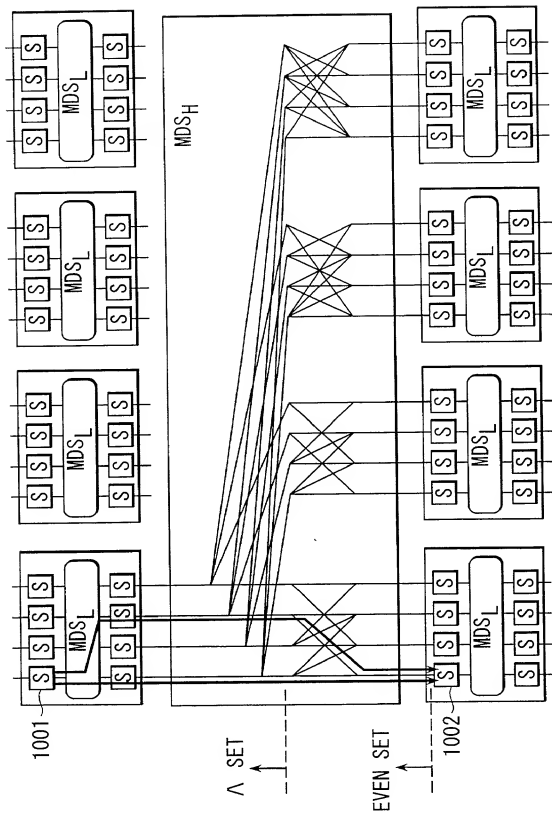


FIG. 35

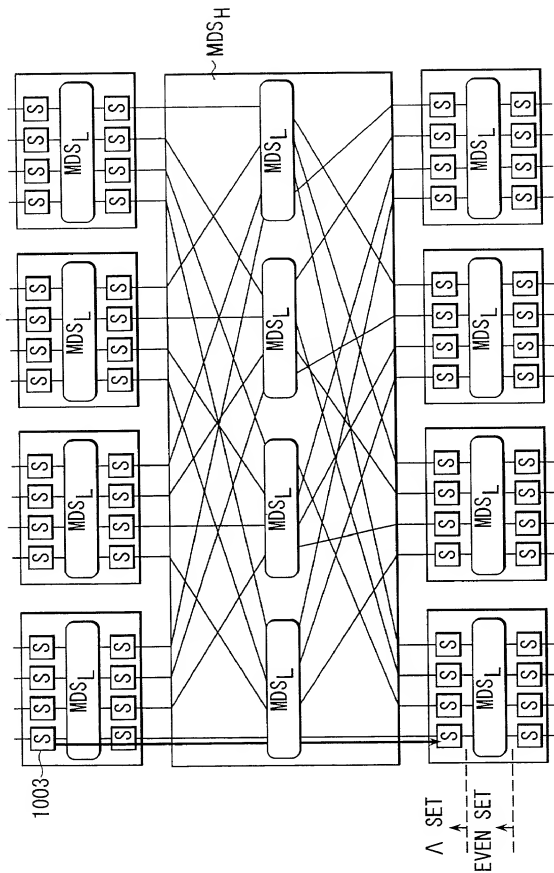


FIG. 36



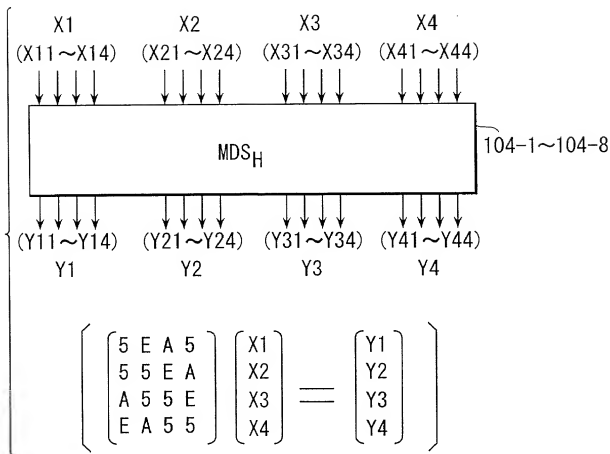


FIG. 37

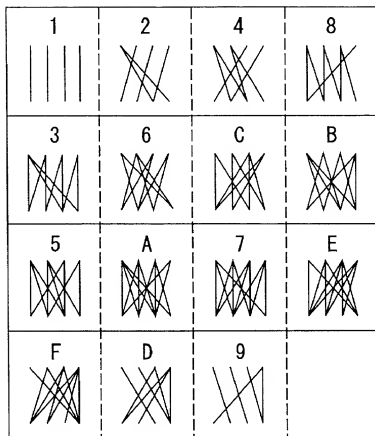


FIG. 38

FIG. 39A

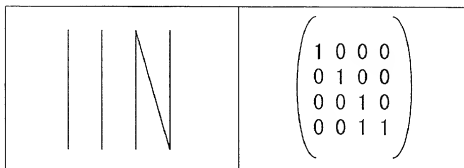


FIG. 39B

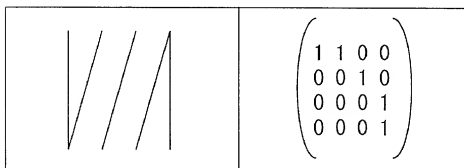


FIG. 39C

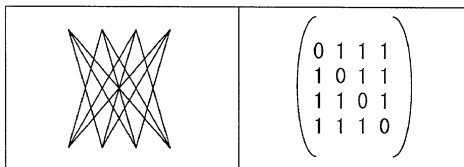
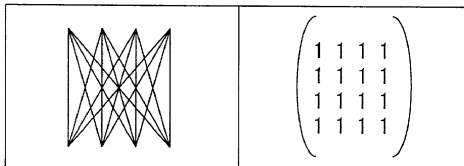


FIG. 39D



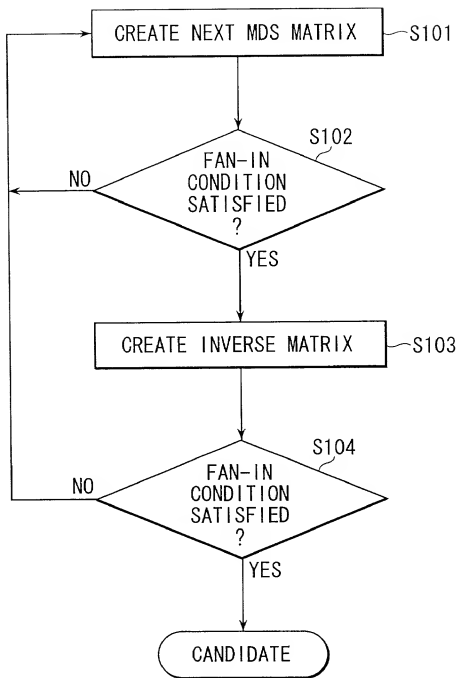


FIG. 40

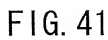


FIG. 41

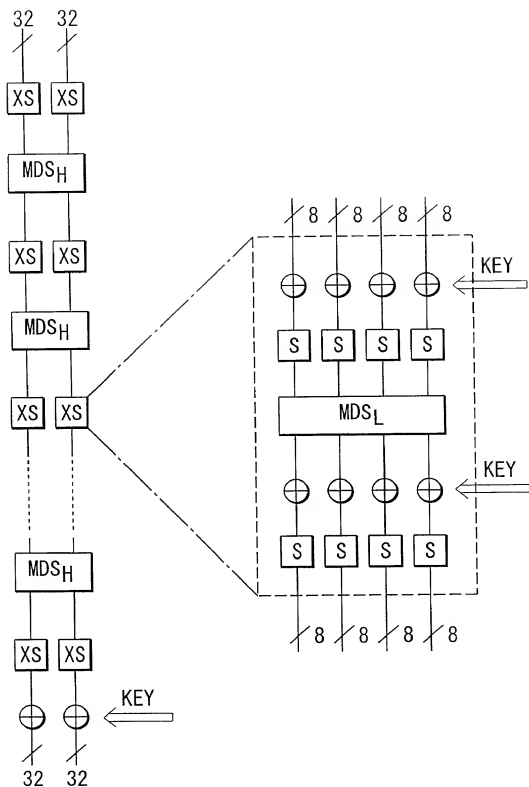


FIG. 42

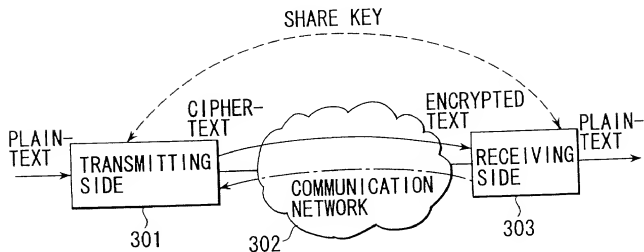


FIG. 43

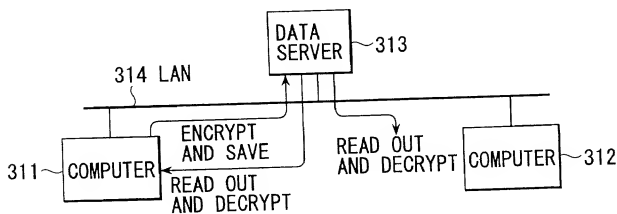


FIG. 44

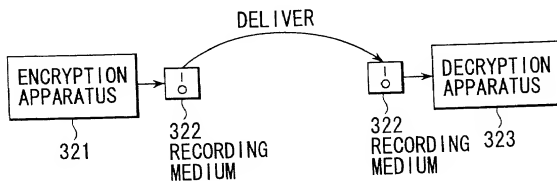


FIG. 45